TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

Expéditeur : L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Destinataire :

voir le formulaire PCT/ISA/220

PCT

OPINION ÉCRITE DE L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

(règle 43*bis*.1 du PCT)

Date d'expédition *(jour/mois/année)* voir le formulaire PCT/ISA/210 (deuxième feuille)

Référence du dossier du déposant ou du mandataire
voir le formulaire PCT/ISA/220

POUR SUITE À DONNER
Voir le point 2 ci-dessous

Demande internationale No.	Date du dépôt international *(jour/mois/année)*	Date de priorité *(jour/mois/année)*
PCT/EP2004/051144	17.06.2004	18.06.2003

Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB
G06F7/72

Déposant
GEMPLUS

1. La présente opinion contient des indications et les pages correspondantes relatives aux points suivants :

- ☒ Cadre n° I Base de l'opinion
- ☐ Cadre n° II Priorité
- ☐ Cadre n° III Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- ☒ Cadre n° IV Absence d'unité de l'invention
- ☒ Cadre n° V Déclaration motivée selon la règle 43*bis*.1(a)(i) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- ☐ Cadre n° VI Certains documents cités
- ☐ Cadre n° VII Irrégularités dans la demande internationale
- ☒ Cadre n° VIII Observations relatives à la demande internationale

2. **SUITE À DONNER**

Si une demande d'examen préliminaire internationale est présentée, la présente opinion sera considérée comme une opinion écrite de l'administration chargée de l'examen préliminaire international, sauf dans le cas où le déposant a choisi une administration différente de la présente administration aux fins de l'examen préliminaire international et que l'administration considérée a notifié au Bureau international, selon la règle 66.1bis.b), qu'elle n'entend pas considérer comme les siennes les opinions écrites de la présente administration chargée de la recherche internationale.

Si, comme cela est indiqué ci-dessus, la présente opinion écrite est considérée comme l'opinion écrite de l'administration chargée de l'examen préliminaire international, le déposant est invité à soumettre à l'administration chargée de l'examen préliminaire international une réponse écrite, avec le cas échéant des modifications, avant l'expiration d'un délai de 3 mois à compter de la date d'envoi du formulaire PCT/ISA/220 ou avant l'expiration d'un délai de 22 mois à compter de la date de priorité, le délai expirant le dernier devant être appliqué.

Pour plus de détails sur les possibilités offertes au déposant, se référer au formulaire PCT/ISA/220.

3. Pour de plus amples détails, se référer aux notes relatives au formulaire PCT/ISA/220.

Nom et adresse postale de l'adminstration chargée de la recherche internationale

Office européen des brevets - P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tél. +31 70 340 - 2040 Tx: 31 651 epo nl
Fax: +31 70 340 - 3016

Fonctionnaire autorisé

Verhoof, P

N° de téléphone +31 70 340-3833

OPINION ÉCRITE DE L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Demande internationale n° PCT/EP2004/051144

Cadre n° I Base de l'opinion

1. En ce qui concerne la **langue**, la présente opinion a été établie sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous ce point.

   ☐ La présente opinion a été établie sur la base d'une traduction de la langue dans laquelle la demande internationale a été déposée dans la langue suivante , qui est la langue de la traduction remise aux fins de la recherche internationale (selon les règles 12.3 et 23.1.b)).

2. En ce qui concerne **la ou les séquences de nucléotides ou d'acides** aminés divulguées dans la demande internationale, le cas échéant, la recherche internationale a été effectuée sur la base des éléments suivants :

   a. Nature de l'élément :

   ☐ un listage de la ou des séquences

   ☐ un ou des tableaux relatifs au listage de la ou des séquences

   b. Type de support :

   ☐ sur papier sous forme écrite

   ☐ sur support électronique sous forme déchiffrable par ordinateur

   c. Moment du dépôt ou de la remise :

   ☐ contenu(s) dans la demande internationale telle que déposée

   ☐ déposé(s) avec la demande internationale, sous forme déchiffrable par ordinateur

   ☐ remis ultérieurement à la présente administration aux fins de la recherche

3. ☐ De plus, lorsque plus d'une version ou d'une copie d'un listage des séquences ou d'un ou plusieurs tableaux y relatifs a été déposée, les déclarations requises selon lesquelles les informations fournies ultérieurement ou au titre de copies supplémentaires sont identiques à celles initialement fournies et ne vont pas au-delà de la divulgation faite dans la demande internationale telle que déposée initialement, selon le cas, ont été remises.

4. Commentaires complémentaires :

OPINION ÉCRITE DE L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Demande internationale n° PCT/EP2004/051144

Cadre n° IV Absence d'unité de l'invention

1. ☒ En réponse à l'invitation (formulaire PCT/ISA/206) à payer des taxes additionnelles, le déposant :

   ☐ a payé des taxes additionnelles.

   ☒ a payé des taxes additionnelles sous réserve.

   ☐ n'a pas payé de taxes additionnelles.

2. ☐ L'administration chargée de la recherche internationale estime qu'il n'est pas satisfait à l'exigence d'unité de l'invention et décide de ne pas inviter le déposant à payer de taxes additionnelles.

3. L'administration chargée de la recherche internationale estime que, aux termes des règles 13.1, 13.2 et 13.3 :

   ☐ il est satisfait à l'exigence d'unité de l'invention

   ☒ il n'est pas satisfait à l'exigence d'unité de l'invention, pour les raisons suivantes :

   voir feuille séparée

4. En conséquence, la présente opinion a été établie à partir des parties suivantes de la demande internationale :

   ☒ toutes les parties de la demande

   ☐ les parties relatives aux revendications nos

Cadre n° V Déclaration motivée selon la règle 43*bis*.1(a)(i) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	5,6,8-11
	Non :	Revendications	1-4,7,12
Activité inventive	Oui :	Revendications	
	Non :	Revendications	5,6,8-11
Possibilité d'application industrielle	Oui :	Revendications	1-12
	Non :	Revendications	

2. Citations et explications

voir feuille séparée

Cadre n° VIII Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :

voir feuille séparée

Concernant le point IV
Absence d'unité de l'invention

Les différentes inventions sont les suivantes :

revendications 1,2,7-12
Procédé sécurisé d'exponentiation dans un groupe noté de façon additive

revendications 3-6
Procédé sécurisé d'exponentiation dans un groupe noté de façon multiplicative

Elles ne sont pas liées entre elles de telle sorte qu'elles ne forment qu'un seul concept inventif général (règle 13.1 PCT), et ce pour les raisons suivantes :

Pour le raisonnement suivant l'art antérieur comme décrit dans XP1061177, cité dans le rapport de recherche, est pris en considération.

Ce document décrit un procédé sécurisé de mise à la puissance dans un groupe additive qui correspond à l'objet de revendication 1. Les revendications 2, 3 et 12, directement dépendantes de revendication 1 forment deux groupes d'inventions, comme indiqué ci-dessus.

XP1061177 se distingue du premier groupe par les caractéristiques 1) et 2c) de la revendication 8, les caractéristiques 2b) de la revendication 9, les caractéristiques 1) et 2c) de la revendication 10, et par les caractéristiques 2b) de la revendication 11. Une éventuelle caractéristique technique spéciale du premier groupe devrait se trouver parmi ces caractéristiques.

XP1061177 se distingue du deuxième groupe par toutes les caractéristiques des revendications 3 à 6. Une éventuelle caractéristique technique spéciale du deuxième groupe devrait se trouver parmi ces caractéristiques.

En comparant les éventuelles caractéristiques techniques spéciales du premier groupe avec celles du deuxième groupe, on constate qu'il n'y peut avoir une caractéristique

technique spéciale en commun entre les deux groupes : Les éventuelles caractéristiques techniques spéciales des deux groupes n'ont aucune caractéristique (identique ou correspondante) en commun. Ces éventuelles caractéristiques techniques spéciales des deux groupes ne renforcent pas mutuellement leurs effet, et ne produisent pas d'interaction non évidente dans le fonctionnement. Les problèmes résolus par les deux groupes de caractéristiques techniques spéciales sont différents.

Par conséquent il y a deux inventions dans la demande, l'une constituée par les revendications 1, 2, 7-12, l'autre par les revendications 3-6.
Ces deux inventions constituent non-unité a posteriori.

Concernant le point V

Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Il est fait référence aux documents suivants dans la présente notification :
   D1 : LIARDET P-Y ET AL: "PREVENTING SPA/DPA IN ECC SYSTEMS USING THE JACOBI FORM" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. 3RD INTERNATIONAL WORKSHOP, CHES 2001, PARIS, FRANCE, 14 - 16 MAY, 2001 PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE, BERLIN: SPRINGER, DE, VOL. 2162, 14 mai 2001 (2001-05-14), pages 391-401, XP001061177 ISBN: 3-540-42521-7
   D2: EP-A-1 296 224 (HITACHI LTD) 26 mars 2003 (2003-03-26)
   D3: US 2003/079139 A1 (DREXLER HERMANN ET AL) 24 avril 2003 (2003-04-24)

2. REVENDICATION INDÉPENDANTE 1

   La présente demande ne remplit pas les conditions énoncées dans l'article 33(1) PCT, l'objet de la revendication 1, dans la mesure où ladite revendication peut être comprise (voir sous point VIII), n'étant pas conforme au critère de nouveauté défini par l'article 33(2) PCT.

2.1 Le document D1 décrit (les références entre parenthèses s'appliquant à ce document)

un procédé de contre-mesure dans un composant électronique mettant en œuvre un algorithme cryptographique à clé publique (page 391, paragraphe 1, alinéa 1), comprenant un calcul d'exponentiation de type gauche-droite (page 393, lignes 1 à 6), de type y=g^d (Q=[k]P) où g (P) et y (Q) sont des éléments du groupe déterminé G (E) noté de façon additive et d (k) est un nombre prédéterminé (implicitement la clé), comprenant une étape de tirage aléatoire ("generating a random element Z' ", page 399, lignes 10,11 ; voir aussi page 392, lignes 5 à 13), au début de l'exécution dudit algorithme d'exponentiation de façon déterministe ou probabiliste, pour masquer l'accumulateur A (Q ; page 393, lignes 1 à 6).

L'objet de la revendication 1, dans la mesure où ladite revendication peut être comprise, n'est donc pas nouveau en vu de D1.

2.2 Le document D3 décrit (les références entre parenthèses s'appliquant à ce document)
un procédé de contre-mesure dans un composant électronique mettant en œuvre un algorithme cryptographique à clé publique (voir paragraphe [0006]), comprenant un calcul d'exponentiation de type gauche-droite (voir paragraphe [0020]), de type y=g^d ($Y=M^d \bmod n$) où g (M) et y (Y) sont des éléments du groupe déterminé G (entiers mod n) noté de façon multiplicative et d (d) est un nombre prédéterminé (clé secrète, voir paragraphe [0005]), comprenant une étape de tirage aléatoire (voir paragraphe [0020], lignes 1 et 2), au début de l'exécution dudit algorithme d'exponentiation de façon déterministe ou probabiliste, pour masquer l'accumulateur A (Z).

L'objet de la revendication 1, dans la mesure où ladite revendication peut être comprise, n'est donc pas nouveau en vu de D3.

3. REVENDICATION INDÉPENDANTE 12

Chacun des documents D1 et D3 décrit de manière fonctionnelle l'appareil correspondant au procédé de la revendication 1. Par conséquent, l'objet de la revendication 12 n'est pas conforme au critère de nouveauté défini par l'Article 33(2) PCT.

4. REVENDICATIONS DÉPENDANTES 2, 7-11

Ces revendications ne contiennent pas de caractéristiques qui, combinées avec les caractéristiques d'une quelconque revendication à laquelle elles se réfèrent, satisfont aux exigences du PCT en matière de nouveauté et d'activité inventive (article 33 2) et 3) PCT) en vu de D1.

Revendication 2: voir point 2.1 ci-dessus;
Revendication 7: voir D1 page 394, ligne 2;
Revendications 8 à 11: voir aussi D2, passages cités dans le rapport de recherche.

5. REVENDICATIONS DÉPENDANTES 3-6

Ces revendications ne contiennent pas de caractéristiques qui, combinées avec les caractéristiques d'une quelconque revendication à laquelle elles se réfèrent, satisfont aux exigences du PCT en matière de nouveauté et d'activité inventive (article 33 2) et 3) PCT) en vu de D3.

Revendications 3 et 4: voir point 2.2 ci-dessus;
Revendications 5 et 6: voir D3 paragraphes [0018] à [0020]

6. POSSIBILITÉ D'APPLICATION INDUSTRIELLE

L'objet des revendications 1-12 concerne le domaine technique de traitement de données cryptographiques et satisfait par conséquent aux critères d'application industrielle (article 33(4) PCT).

Concernant le point VIII
Certaines observations relatives à la demande internationale

Selon la revendication 1 le groupe déterminé G est noté de façon multiplicative. Par contre, selon la revendication 2, qui dépend de la revendication 1, le groupe déterminé G est noté de façon additive. Un groupe G noté à la fois de façon multiplicative et additive n'a pas été exposé. Cette discordance entre la revendication 1 et la revendication 2 engendre un doute quant à l'étendue de la protection demandée, au point que ces revendications

deviennent obscures.

Dans l'analyse d'unité de invention sous point IV et la déclaration motivée sous point V, la plus large interprétation possible de ces revendications a été adoptée, supposant que dans la revendication 1 le groupe déterminé G est noté de façon multiplicative ou additive.